A NEW LOOK AT HECKE'S INDEFINITE THETA SERIES

A. POLISHCHUK

This note is devoted to the q-series of the form

$$\sum_{m\geq 0,n\geq 0} f(m,n)q^{Q(m,n)} - \sum_{m<0,n<0} f(m,n)q^{Q(m,n)}$$

where Q is an indefinite quadratic form on $\mathbb{Z}^2$, $f(m,n)$ is a doubly periodic function on $\mathbb{Z}^2$ such that the sums of $f(m,n)q^{Q(m,n)}$ over all vertical and all horizontal lines in $\mathbb{Z}^2$ vanish. Some of these series appeared as coefficients in univalued triple Massey products on elliptic curves computed via homological mirror symmetry in [3]. In particular, in this context the condition of vanishing of sums over vertical and horizontal lines appears to be related to the standard necessary condition of the existence of triple Massey products (the vanishing of two double products). In the present paper we generalize Theorem 3 of [3] which relates such series to the indefinite theta series considered by Hecke in [1], [2] (our approach is completely elementary and doesn't use the connection with triple products on elliptic curves). The main consequence of this relation is the modularity of our q-series. We also show that the problem of finding all linear relations between our series is related to the study of orbits of actions of dihedral groups on $(\mathbb{Z}/N\mathbb{Z})^2$.

1. Main result

1.1. **Hecke's indefinite theta series.** Let us recall the definition of these series. Let K be a totally real quadratic extension of $\mathbb{Q}$, i.e. K is either a field of the form $\mathbb{Q}(\sqrt{D})$ (where $D > 0$) or the algebra $\mathbb{Q}\oplus\mathbb{Q}$. We have the norm map $\mathrm{Nm} : K \to \mathbb{Q}$ (in case of $\mathbb{Q}\oplus\mathbb{Q}$ this is the product of components). Let us denote by $C \subset K$ the set of elements with positive norm. The cone C is a union of two components and we define the function $\mathrm{sign} : C \to \pm 1$ which assigns value 1 (resp. -1) on totally positive (resp. negative) elements (in the case of $\mathbb{Q}\oplus\mathbb{Q}$ "total positivity" means positivity of both components). Let us denote by $U_+(K)$ the subgroup of the multiplicative group K consisting of totally positive elements $k \in K^*$ with norm 1 (in the case of $\mathbb{Q}\oplus\mathbb{Q}$ this is the group of elements (r, r^{-1}) where $r > 0$). Note that the group of $\mathbb{Q}$-linear automorphisms of K preserving Nm decomposes as follows:

$$\mathrm{Aut}_{\mathbb{Q}}(K, \mathrm{Nm}) = \pm\,\mathrm{id} \times U_+(K) \times \mathrm{Gal}(K/\mathbb{Q})$$

where $U_+(K)$ acts on K by multiplication. Let $\Lambda \subset K$ be a lattice (i.e. a $\mathbb{Z}$-submodule of rank 2), $\Lambda + c$ be a coset for this lattice (where $c \in K$). Hecke's indefinite theta series is

$$\Theta_{\Lambda,c} = \sum_{\lambda\in(\Lambda+c)\cap C/G} \mathrm{sign}(\lambda)q^{d\cdot \mathrm{Nm}(\lambda)}$$

This work was partially supported by NSF grant.

where G is the subgroup in $U_+(K)$ consisting of the elements preserving $\Lambda + c$, d is a positive rational number such that $d\,\mathrm{Nm}$ takes integer values on $\Lambda + c$. Hecke proved that this series is modular of weight 1 for the subgroup $\Gamma_0(n) \subset \mathrm{SL}_2(\mathbb{Z})$ with some explicit level n. [1] Note that the elements of $U_+(K)$ preserving Λ are totally positive units, hence, G is an infinite cyclic group. In particular, if we replace in the above definition G by any infinite subgroup in $U_+(K)$ preserving $\Lambda + c$ the resulting series will be an integral multiple of $\Theta_{\Lambda,c}$.

1.2. **Formulation of the main theorem.** *Let $Q(m,n) = am^2 + 2bmn + cn^2$ be a $\mathbb{Q}$-valued indefinite quadratic form on $\mathbb{Z}^2$ (so $b^2 > ac$) which is positive on the cone $mn \geq 0$ (i.e. a, b and c are positive). Let $f(m,n)$ be a doubly periodic complex-valued function on $\mathbb{Z}^2$ (so $f(m+N,n) = f(m,n+N) = f(m,n)$ for some $N > 0$). Assume that for all m_0 and n_0 one has*

$$\sum_{m\in\mathbb{Z}} f(m,n_0)q^{Q(m,n_0)} = \sum_{n\in\mathbb{Z}} f(m_0,n)q^{Q(m_0,n)} = 0$$

(i.e. all sums along horizontal and vertical lines are zero). Assume also that Q takes integer values on the support of f. Then the series

$$\Theta_{Q,f} = \sum_{m\geq 0, n\geq 0} f(m,n)q^{Q(m,n)} - \sum_{m<0,n<0} f(m,n)q^{Q(m,n)}$$

is modular of weight 1.

Moreover, the space of modular forms of weight 1 spanned by these series coincides with the space generated by Hecke's indefinite theta series.

1.3. **Proof.** Our first task is to unravel the condition that the sums along horizontal and vertical lines are zero. Let us extend the function $f(m,n)$ from $\mathbb{Z}^2$ to $\mathbb{Q}^2$ by zero. Then we claim that this condition is equivalent to the following two identities:

$$f(m,n) = -f(-\frac{2b}{a}n - m, n),$$

$$f(m,n) = -f(m, -\frac{2b}{c}m - n).$$

Indeed, this follows from the fact that Q restricted to a vertical or horizontal line assumes each value at exactly two points (sometimes coinciding, in which case the coefficient should be zero), so in order for the sum to be zero the corresponding coefficients should cancel out. Let us consider the following two operators preserving Q:

$$A = \begin{pmatrix} -1 & p \\ 0 & 1 \end{pmatrix},$$

$$B = \begin{pmatrix} 1 & 0 \\ r & -1 \end{pmatrix}.$$

where $p = -\frac{2b}{a}$, $r = -\frac{2b}{c}$. Then the conditions on f can be rewritten as

$$f(Ax) = f(Bx) = -f(x) \tag{1.1}$$

for every $x \in \mathbb{Q}^2$. Let $S \subset \mathbb{Z}^2 \subset \mathbb{Q}^2$ be the support of f. We can assume that $f \neq 0$ so that S is non-empty. Let $\Lambda = \{x \in \mathbb{Q}^2 : \ S + x = S\}$. Since f is doubly periodic, Λ is a sublattice of $\mathbb{Z}^2$. On the other hand, both operators A and B preserve S,

[1] In the original definition of Hecke Λ was an ideal in the ring of integers, however, the same proof works for any lattice. Also, Hecke makes a concrete choice of d. For our purposes it is more convinient to allow any d such that $d\,\mathrm{Nm}$ takes integer values on $\Lambda + c$.

hence, they preserve Λ. It follows that $\mathrm{Tr}(AB)=-2+rp$ is an integer, i.e. $rp=\frac{4b^2}{ac}$ is an integer.

Making the change of variables of the form $m=m'/m_0$, $n=n'/n_0$, where m_0 and n_0 are positive integers such that $\frac{m_0}{n_0}=\frac{a}{2b}$, we can always assume that $a=2b$. Then the above condition will imply that both matrices A and B have integer coefficients. In particular, we can consider them acting on $(\mathbb{Z}/N\mathbb{Z})^2$, where N is the (double) period of f. Let us denote by G_N the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ generated by these two operators (by abuse of notation we will denote the corresponding elements of G_N also by A and B). Note that $A^2=B^2=1$, so G_N is actually a dihedral group. Now clearly the space of functions f on $(\mathbb{Z}/N\mathbb{Z})^2$ satisfying the condition (1.1) is spanned by functions supported on orbits of G_N (and satisfying (1.1)). Let $O\subset(\mathbb{Z}/N\mathbb{Z})^2$ be an orbit of G_N, f be a function on O satisfying (1.1). In order for f to be non-zero the orbit O should satisfy the following condition: for every $x\in O$ one has $Ax\neq x$, $Bx\neq x$. Let us call such orbit *admissible*. Conversely, it is easy to see that for every admissible orbit O there is a unique (up to a constant) function f on O satisfying (1.1). Indeed, let $\chi:G_N\to\{\pm1\}$ be the character defined by $\chi(A)=\chi(B)=-1$. Then the orbit is admissible if and only if χ is trivial on the stabilizer subgroup of a point in O (since every element $g\in G_N$ with $\chi(g)=-1$ is conjugate either to A or to B). Thus, for every admissible orbit $O=Gx$ we can define the function f_O on O by setting $f_O(gx)=\chi(g)$ (up to a sign f_O doesn't depend on x). It suffices to deal with the series associated with such functions. So, in the rest of the proof we will assume that f is a doubly periodic function on $\mathbb{Z}^2$ with values ±1 satisfying (1.1). Let $S\subset\mathbb{Z}^2\subset\mathbb{Q}^2$ be the support of f. Then $S=S_1\cup S_{-1}$ where $S_1=f^{-1}(1)$, $S_{-1}=f^{-1}(-1)$. Furthermore, we have $AS_1=BS_1=S_{-1}$. Let K be the quadratic extension of $\mathbb{Q}$ associated with the form Q. If $D=b^2-ac$ is not a complete square then K is a real quadratic field $\mathbb{Q}(\sqrt{D})$, otherwise, $K=\mathbb{Q}\oplus\mathbb{Q}$. The usual notation $x+y\sqrt{D}$ for elements of a real quadratic field K can be extended to the case when D is a complete square and $K=\mathbb{Q}\oplus\mathbb{Q}$. Namely, in this case we set $x+y\sqrt{D}:=(x+y\sqrt{D},x-y\sqrt{D})$. We have

$$Q(m,n)=\frac{1}{c}[(bm+nc)^2-Dm^2]=\frac{1}{c}\,\mathrm{Nm}(bm+nc+m\sqrt{D}).$$

Thus, it makes sense to consider $\mathbb{Z}^2$ as a lattice in K via the map $(m,n)\mapsto(bm+nc+m\sqrt{D})$. For two non-zero elements $k_1,k_2\in K$ let us denote $\langle k_1,k_2\rangle=\mathbb{Q}_{>0}k_1+\mathbb{Q}_{>0}k_2$, $[k_1,k_2]=\mathbb{Q}_{\geq0}k_1+\mathbb{Q}_{\geq0}k_2$, $\langle k_1,k_2]=\mathbb{Q}_{\geq0}k_1+\mathbb{Q}_{>0}k_2$. Using this notation we can write

$$\Theta_{Q,f}=\sum_{\lambda\in S_1\cap[1,b+\sqrt{D}]}q^{\frac{\mathrm{Nm}(\lambda)}{c}}-\sum_{\lambda\in S_1\cap\langle-1,-b-\sqrt{D}\rangle}q^{\frac{\mathrm{Nm}(\lambda)}{c}}-\sum_{\lambda\in S_{-1}\cap[1,b+\sqrt{D}]}q^{\frac{\mathrm{Nm}(\lambda)}{c}}+\sum_{\lambda\in S_{-1}\cap\langle-1,-b-\sqrt{D}\rangle}q^{\frac{\mathrm{Nm}(\lambda)}{c}}.$$

Let us extend the operators A and B from our lattice to K by $\mathbb{Q}$-linearity. We have $B(1)=-1$, $B(b+\sqrt{D})=-b+\sqrt{D}$. Therefore, making the change of variables $\lambda\mapsto B\lambda$ in the last two sums we get

$$\sum_{\lambda\in S_{-1}\cap[1,b+\sqrt{D}]}q^{\frac{\mathrm{Nm}(\lambda)}{c}}=\sum_{\lambda\in S_1\cap[-1,-b+\sqrt{D}]}q^{\frac{\mathrm{Nm}(\lambda)}{c}},$$

$$\sum_{\lambda\in S_{-1}\cap\langle -1,-b-\sqrt{D}\rangle} q^{\frac{\mathrm{Nm}(\lambda)}{c}} = \sum_{\lambda\in S_1\cap\langle 1,b-\sqrt{D}\rangle} q^{\frac{\mathrm{Nm}(\lambda)}{c}}.$$

Hence, we can rewrite $\Theta_{Q,f}$ as follows:

$$\Theta_{Q,f} = \sum_{\lambda\in S_1\cap\langle b-\sqrt{D},b+\sqrt{D}]} q^{\frac{\mathrm{Nm}(\lambda)}{c}} - \sum_{\lambda\in S_1\cap[-b+\sqrt{D},-b-\sqrt{D}\rangle} q^{\frac{\mathrm{Nm}(\lambda)}{c}}.$$

Now it is easy to check that the operator $AB : K \to K$ coincides with multiplication by the element $\frac{b+\sqrt{D}}{b-\sqrt{D}}$ of norm 1. Therefore, we have

$$\Theta_{Q,f} = \sum_{\lambda\in S_1\cap C/G} \mathrm{sign}(\lambda) q^{\frac{\mathrm{Nm}(\lambda)}{c}},$$

where G is the infinite cyclic group generated by AB. Note that the set S_1 is a union of a finite number of cosets $(\Lambda_1 + x_i, i = 1,\ldots,s)$ for the lattice $\Lambda_1 = \{x \in K : S_1 + x = S_1\}$. Furthermore, since Λ_1 is preserved by the action of G, there is a subgroup of finite index $G_0 \subset G$ preserving each of these cosets. Then we have

$$[G : G_0]\Theta_{Q,f} = \sum_{\lambda\in S_1\cap C/G_0} \mathrm{sign}(\lambda) q^{\frac{\mathrm{Nm}(\lambda)}{c}} = \sum_{i=1}^{s} \sum_{\lambda\in(\Lambda_1+x_i)\cap C/G_0} \mathrm{sign}(\lambda) q^{\frac{\mathrm{Nm}(\lambda)}{c}}.$$

Now each of the terms is a scalar multiple of Hecke's series.

Conversely, assume that we are given a lattice $\Lambda \subset K$ in a totally real quadratic extension of $\mathbb{Q}$ and a coset $\Lambda + c$. Let $G \subset U_+(K)$ be the subgroup preserving $\Lambda + c$. Recall that G is an infinite cyclic group. Let ϵ be a generator of G. Let us define the $\mathbb{Q}$-linear operators A and B on K as follows: $B(x) = -\overline{x}$ where $\overline{x}$ is the conjugate element to x (in the case $K = \mathbb{Q}\oplus\mathbb{Q}$ and $x = (x_1, x_2)$ one has $\overline{x} = (x_2, x_1)$), $A(x) = -\epsilon\cdot\overline{x}$. Note that $A^2 = B^2 = 1$ while $\det A = \det B = -1$. Let $k \in K$ be an eigenvector for A with eigenvalue -1, so that $\epsilon\overline{k} = k$. Changing k by $-k$ if necessary we can assume that k is totally positive. Then we have

$$\Theta_{\Lambda,c} = \sum_{\lambda\in(\Lambda+c)\cap C/G} \mathrm{sign}(\lambda) q^{d\cdot\mathrm{Nm}(\lambda)} = \sum_{\lambda\in(\Lambda+c)\cap[k,\overline{k}\rangle} q^{d\cdot\mathrm{Nm}(\lambda)} - \sum_{\lambda\in(\Lambda+c)\cap\langle -k,-\overline{k}]} q^{d\cdot\mathrm{Nm}(\lambda)}.$$

Note that we have $1 \in \langle k, \overline{k}\rangle$ since k is totally positive. Therefore, we can split each of the above sums into two according to decompositions $[k,\overline{k}\rangle = [k,1]\bigsqcup\langle 1,\overline{k}\rangle$, $\langle -k,-\overline{k}] = \langle -k,-1\rangle\bigsqcup[-1,-\overline{k}]$. Making the change of variable $\lambda \mapsto B(\lambda)$ in the sums over $\langle 1,\overline{k}\rangle$ and over $[-1,-\overline{k}]$ we can rewrite the above sum as follows:

$$\Theta_{\Lambda,c} = \sum_{\lambda\in S\cap([1,k]\cup\langle -k,-1\rangle)} f(\lambda)\,\mathrm{sign}(\lambda) q^{d\cdot\mathrm{Nm}(\lambda)},$$

where $S = (\Lambda + c) \cup B(\Lambda + c)$, the function f supported on S is defined by

$$f(x) = \delta_{\Lambda+c}(x) - \delta_{B(\Lambda+c)}(x)$$

where δ_I is the characteristic function of the set I. Note that since the operator AB preserves $\Lambda + c$ and $(AB)B = B(AB)^{-1}$, it also preserves $B(\Lambda + c)$, hence, $f(ABx) = f(x)$. On the other hand, by definition $f(Bx) = -f(x)$. Therefore, we also have $f(Ax) = -f(x)$. Now taking the coordinates with respect to the basis $(1, k)$ as variables of summation we see that the above series assumes the form

$$\sum_{(m,n)\in S,m\geq 0,n\geq 0} f(m,n)q^{Q(m,n)} - \sum_{(m,n)\in S,m<0,n<0} f(m,n)q^{Q(m,n)}$$

where S is a finite union of cosets with respect to some $\mathbb{Z}$-lattice in $\mathbb{Q}^2$, f is a periodic function on S with the property that sums of $f(m,n)q^{Q(m,n)}$ over all vertical and horizontal lines are zero. It remains to change variables (m,n) to (Mm,Mn) where $MS \subset \mathbb{Z}^2$ to rewrite this series in the form we require. $\square$

2. Remarks and examples

2.1. **Linear relations.** The series $\Theta_{Q,f}$ is often equal to zero. It is an important open problem to formulate the necessary and sufficient conditions for it to be zero. In other words, the problem is to describe all linear relations between such series for some basis in the space of functions f satisfying the assumptions of the main theorem. We restrict ourself to several observations. As above we assume that $p = -2b/a$ and $r = -2b/c$ are integers, so that we have an action of operators A and B on $\mathbb{Z}^2$ preserving the form Q. In the course of proof of the main theorem we introduced the subgroup $G_N \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ generated by these two operators modulo N. As we have seen above the space of functions on $(\mathbb{Z}/N\mathbb{Z})^2$ satisfying the condition (1.1) (further called *admissible* functions) has a basis (f_O) enumerated by admissible G_N-orbits. The change of variables $(m,n) \mapsto (-m,-n)$ shows that

$$\Theta_{Q,f} = -\Theta_{Q,f\circ[-1]},$$

where $f \circ [-1](m,n) = f(-m,-n)$. Let us call an admissible orbit O *symmetric* if $-O = O$, and *asymmetric* otherwise. Note that for an asymmetric orbit one has $O \cap -O = \emptyset$. For every symmetric orbit O the corresponding function f_O is either even or odd. We call a symmetric orbit O *even* (resp. *odd*) if f_O is even (resp. odd). Now the above equation shows that for an even symmetric orbit O one has $\Theta_{Q,f_O} = 0$, while for an asymmetric orbit O one has $\Theta_{Q,f_O} = \pm\Theta_{Q,f_{-O}}$ (the sign comes from the sign ambiguity in the definition of f_O).

The action of the operator $\tau : (m,n) \mapsto (n,m)$ gives some additional relations between Θ_{Q,f_O}. Indeed, for any Q we have

$$\Theta_{Q,f} = \Theta_{Q\circ\tau,f\circ\tau}.$$

If $Q \circ \tau = Q$ (i.e. $a = c$) then for every admissible orbit O we have $f_O \circ \tau = \pm f_{O'}$ for some other admissible orbit O', hence $\Theta_{Q,f_O} = \pm\Theta_{Q,f_{O'}}$. In particular, if $f_O \circ \tau = -f_O$ then $\Theta_{Q,f_O} = 0$.

Finally, we can make the changes of variables $(m,n) \mapsto (t_1 m, t_2 n)$, where t_1 and t_2 are positive rational numbers, in the case when this transformation sends the support of f into $\mathbb{Z}^2$. This transformation will always change the form Q (unless $t_1 = t_2 = 1$). However, combining it with the operator τ with respect to the new variables we can derive more linear relations for fixed Q (generalizing the above relations for the case $a = c$). Namely, assume that $c/a = t^2$ for some positive rational number t. Then the operator

$$\tau_t : (m,n) \mapsto (tn, t^{-1}m)$$

preserves Q and satisfies $\tau_t^2 = 1$, $\tau_t A = B\tau_t$. In particular if f is an admissible function such that τ_t sends the support of f into $\mathbb{Z}^2$ then $f \circ \tau_t$ is also admissible (perhaps with a different double period) and we have $\Theta_{Q,f\circ\tau_t} = \Theta_{Q,f}$.

We were not able to find any other linear relations between the series $(\Theta_{Q,f})$ for fixed Q. However, at present we are far from proving that these are all relations. Even the non-vanishing of Θ_{Q,f_O} for odd symmetric and for asymmetric admissible G_N-orbits (in the case when a/c is not a square in $\mathbb{Q}$) is still an open problem.

Note that some non-vanishing results were proven in [3] using homological mirror symmetry.

In Hecke's paper one can find the following vanishing condition for an indefinite theta series $\Theta_{\Lambda,c}$ (see [2], Satz 1): if there exists a totally negative element $\delta \in K^*$ with $\mathrm{Nm}(\delta) = 1$ such that $\delta(\Lambda + c) = \Lambda + c$ then $\Theta_{\Lambda,c} = 0$. Let us show that this vanishing is actually one of the linear relations considered above. We will use the notation introduced in the proof of the main theorem. Let (Q, f) be the data constructed in the second half of the proof so that $\Theta_{\Lambda,c} = \Theta_{Q,f}$. First of all, notice that $\delta^2 \in G$, hence $\delta^2 = \epsilon^n$ for some integer n. Changing δ by a power of ϵ we can assume that either $\delta^2 = 1$ or $\delta^2 = \epsilon$. In the former case $\delta = -1$ so one has $f \circ [-1] = f$. In the latter case we have $\epsilon\overline{\delta} = \delta$, so rescaling k we can assume that $k = -\delta$. It is easy to see that the operator $\delta B : x \mapsto -\delta\overline{x}$ preserves Nm and switches 1 and k, as well as $\Lambda + c$ and $B(\Lambda + c)$. Hence, the transposition $\tau : (m, n) \mapsto (n, m)$ preserves Q and satisfies $f \circ \tau = -f$. A different choice of k would lead to a similar relation with S replaced by τ_t.

2.2. **Symmetric orbits.** Henceforward, operators A and B are always considered modulo N. In the situation when the subgroup $G_N \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ $(N > 2)$ contains the matrix $-\mathrm{id}$ every orbit is symmetric. Furthermore, since the character $\chi : G_N \to \{\pm 1\}$ defined by $\chi(A) = \chi(B) = -1$ coincides with $\det|_{G_N}$, we have $\chi(-\mathrm{id}) = 1$, hence every orbit is even. Thus, we get $\Theta_{Q,f} = 0$ for all admissible f. The following proposition gives a criterion allowing to recognize this situation in the case when N is an odd prime.

Proposition 2.1. *Assume that N is an odd prime. Then $-\mathrm{id} \in G_N$ if and only if $rp \mod N$ is of the form $2 + \lambda + \lambda^{-1}$ where λ is an element of even order in $\mathbb{F}^*_{N^2}$ ($\mathbb{F}_{N^2}$ is the finite field of cardinality N^2). The number of such residues modulo N is equal to $N - \frac{n_1+n_2}{2}$ where n_1 (resp. n_2) is the maximal odd divisor of $N - 1$ (resp. $N + 1$).*

Proof. Since $G_N \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is generated by AB the condition $-\mathrm{id} \in G_N$ is equivalent to $(AB)^n = -\mathrm{id}$ for some n. We have $\mathrm{Tr}(AB) = rp - 2$, $\det(AB) = 1$, so the eigenvalues λ_1, λ_2 of AB are roots of the equation

$$\lambda^2 - (rp - 2)\lambda + 1 = 0.$$

Assume first that $\lambda_1 = \lambda_2$. Then either $rp = 4$ or $rp = 0$. In the former case $\lambda_1 = \lambda_2 = 1$, hence, no power of AB equals $-\mathrm{id}$. In the latter case one can easily check that $(AB)^N = -\mathrm{id}$. On the other hand, 0 can be represented in the form $2 + \lambda + \lambda^{-1}$ for $\lambda = -1$.

Now assume that $\lambda_1 \neq \lambda_2$. Then the condition $(AB)^n = -\mathrm{id}$ is equivalent to $\lambda_1^n = -1$, i.e. λ_1 has even order in the multiplicative group of $\overline{\mathbb{F}}_N$. It remains to notice that $\lambda_1 \in \mathbb{F}^*_{N^2}$ and that we have $rp - 2 = \lambda_1 + \lambda_1^{-1}$.

To compute the number of such residues modulo N we note that the condition $\lambda + \lambda^{-1} \in \mathbb{F}_N$ means that either $\lambda^{N-1} = 1$ or $\lambda^{N+1} = 1$. The number of elements λ of even order such that $\lambda^m = 1$ (where m is either $N - 1$ or $N + 1$) is equal to $m - n$ where n is the maximal odd divisor of m. Therefore, the number of elements in $\mathbb{F}_N$ of the form $\lambda + \lambda^{-1}$ is equal to

$$1 + \frac{(N-1) - n_1 - 1}{2} + \frac{(N+1) - n_2 - 1}{2} = N - \frac{n_1 + n_2}{2}.$$

$\square$

Taking in the above proposition λ to be -1, ζ_4 and ζ_6 (where ζ_l is a primitive root of unity of order l) we get $rp \equiv 0 \mod (N)$, $rp \equiv 2 \mod (N)$ and $rp \equiv 3 \mod (N)$ respectively. On the other hand, we claim that if $rp \equiv 1 \mod (N)$ or $rp \equiv 4 \mod (N)$ then $-\mathrm{id} \notin G_N$. Indeed, the equation $4 = 2 + \lambda + \lambda^{-1}$ has the only solution $\lambda = 1$ while the solutions of the equation $1 = 2 + \lambda + \lambda^{-1}$ are roots of unity of order 3. These are the only cases of the above criterion which are independent of N. Here are the lists of values of $rp \mod (N)$ such that $-\mathrm{id} \notin G_N$ for small odd primes N:
$N = 3$: $rp \equiv 1 \mod (3)$;
$N = 5$: $rp \equiv 1, 4 \mod (5)$;
$N = 7$: $rp \equiv 1, 4 \mod (7)$;
$N = 11$: $rp \equiv 1, 4, 5, 9 \mod (11)$.
$N = 13$: $rp \equiv 1, 4, 9, 10, 12 \mod (13)$.

Our last general observation is that in the case when N is an odd prime, all symmetric G_N-orbits have the same parity, i.e. they are either all odd or all even.

Proposition 2.2. *Assume that N is an odd prime. Then either $-\mathrm{id} \in G_N$ or every symmetric G_N-orbit is odd.*

Proof. Assume that there exists a non-zero vector $v \in (\mathbb{Z}/N\mathbb{Z})^2$ and an element $g \in G_N$ such that $gv = -v$ and $\det(g) = 1$. Then both eigenvalues of g are -1, hence, $g^N = -\mathrm{id}$. □

2.3. **Examples.** In all examples below we assume that a, c, $p = -\frac{2b}{a}$ and $r = -\frac{2b}{c}$ are integers (b is a half-integer). Note that we are interested only in the cases when G_N doesn't contain $-\mathrm{id}$. In particular, if N is an odd prime we can assume that $rp \not\equiv 0 \mod (N)$. In this case the conjugacy class of the subgroup $G_N \subset \mathrm{GL}_2(\mathbb{Z}/N)^2$ depends only on $rp \mod (N)$. For instance, if $rp \equiv 1 \mod (N)$ then G_N is isomorphic to the permutation group S_3. In examples 1 and 2 below we consider in details cases $N = 3$ and $N = 5$. It turns out that in these cases all admissible orbits are symmetric (they are automatically odd by proposition 2.2). The simplest example of an asymmetric admissible orbit (for prime N) occurs for $N = 7$ (see example 3 below).
1. $N = 3$, $rp \equiv 1 \mod (3)$. Then there is a unique admissible orbit: the orbit of $(1, 0)$. For $r \equiv p \equiv 1 \mod (3)$ (resp. $r \equiv p \equiv -1 \mod (3)$) the corresponding admissible function is $f(m, n) = \chi_3(m+n)$ (resp. $f(m, n) = \chi_3(m-n)$) where χ_3 is the non-trivial Dirichlet character modulo 3 such that $\chi_3(\pm 1) = \pm 1$. Let us assume that $a \leq c$ (we can always achieve this using the transformation $(m, n) \mapsto (n, m)$ if necessary). Then we have

$$\Theta_{Q,f} \equiv q^a + \chi_3(r)q^c \mod (q^{a+1}).$$

It follows that this theta series doesn't vanish unless $r \equiv -1 \mod (3)$ and $a = c$. In the latter case we have $Q(n, m) = Q(m, n)$ while $f(n, m) = -f(m, n)$ so that $\Theta_{Q,f} = 0$.
2. $N = 5$.
(a) $rp \equiv 1 \mod (5)$. In this case there are two distinct admissible orbits: the orbit of $(1, 0)$ and the orbit of $(2, 0)$. It is easy to see that unless $a = c$ the corresponding two theta functions Θ_{Q,f_1} and Θ_{Q,f_2} are linearly independent. More precisely, the initial terms of these series look as follows (in (i) and (ii) we assume that $a \leq c$):

(i)$p \equiv r \equiv 1(5)$:

$$\Theta_{Q,f_1} \equiv q^a + q^c \mod (q^{a+1}),\ \Theta_{Q,f_2} \equiv q^{4a} + q^{4c} \mod (q^{4a+1}).$$

(ii)$p \equiv r \equiv -1(5)$:

$$\Theta_{Q,f_1} \equiv q^a - q^c \mod (q^{a+1}),\ \Theta_{Q,f_2} \equiv q^{4a} - q^{4c} \mod (q^{4a+1}).$$

(iii)$p \equiv 2(5)$, $r \equiv -2(5)$:

$$\Theta_{Q,f_1} \equiv q^a - q^{4c} \mod (q^{\min(a,4c)+1}),\ \Theta_{Q,f_2} \equiv q^c - q^{4a} \mod (q^{\min(4a,c)+1}).$$

Furthermore, in the case $a = 4c$ we have

$$\Theta_{Q,f_1} \equiv q^{9c} \mod (q^{9c+1})$$

while in the case $c = 4a$ we have

$$\Theta_{Q,f_2} \equiv q^{9a} \mod (q^{9a+1}).$$

If $a = c$ then in the case (ii) we have $\Theta_{Q,f_1} = \Theta_{Q,f_2} = 0$ while in the case (iii) we have $\Theta_{Q,f_2} = \Theta_{Q,f_1}$.

(b) $rp \equiv -1 \mod (5)$. In this case AB has order 5 but there are still two admissible orbits: the orbit of $(1,0)$ and the orbit of $(2,0)$.[2] The analysis of the initial terms of these series (very similar to the case (a)) implies that the corresponding two theta series are linearly independent unless $a = c$.

3. $N = 7$, $r \equiv p \equiv 1 \mod (7)$. There are 5 admissible orbits: 3 symmetric orbits and 2 asymmetric orbits. The symmetric orbits are $O_1 = G_N \cdot (1,0)$, $2 \cdot O_1$, and $3 \cdot O_1$. The asymmetric orbits are $O_2 = G_N \cdot (1,3)$ and $-O_2$. Using the relation $\Theta_{Q,f_{-O_2}} = -\Theta_{Q,f_{O_2}}$ we can exclude the orbit $-O_2$ from our consideration. The initial terms of the remaining 4 theta series look as follows (assuming that $a \le c$)

$$\Theta_{Q,f_{O_1}} \equiv q^a + q^c \mod (q^{a+1}),$$

$$\Theta_{Q,f_{2O_1}} \equiv q^{4a} + q^{4c} \mod (q^{4a+1}),$$

$$\Theta_{Q,f_{3O_1}} \equiv q^{9a} + q^{9c} \mod (q^{9a+1}),$$

$$\Theta_{Q,f_{O_2}} \equiv q^{9a+c+6b} + q^{a+9c+6b} \mod (q^{9a+c+6b+1}).$$

This immediately implies that they are linearly independent.

4. The indefinite theta series considered in Theorem 2 of [3] correspond to the following situation. Let us assume that $\frac{b}{a}$ and $\frac{b}{c}$ are integers (not just half-integers as before). In this case the discriminant $D = b^2 - ac$ is divisible by ac. We are going to take $N = \frac{4D}{ac}$. Let s_1 and s_2 be arbitrary odd numbers. It is easy to check that the G_N-orbit of the element

$$v_{s_1,s_2} = (\frac{b}{a}s_2 - s_1, \frac{b}{c}s_1 - s_2) \in (\mathbb{Z}/N\mathbb{Z})^2$$

is admissible and consists of four elements which are congruent to v_{s_1,s_2} modulo $N/2$. On the other hand, if l divides $\frac{b}{a}+1$ and $\frac{b}{c}+1$ then $\frac{D}{ac}$ is divisible by l and the $2l$-torsion element $v_l = \frac{2D}{lac}(1,1) \in (\mathbb{Z}/N\mathbb{Z})^2$ is G_N-invariant. The series considered in [3] correspond to the orbits of the elements $v_{s_1,s_2} + t \cdot v_l$ where $t \in \mathbb{Z}$ (these orbits depend only on $t \mod (l)$).

[2]In this case A and B have a common invariant vector which allows to have bigger admissible orbits than in case (a).

References

[1] E. Hecke, *Über einen neuen Zusammenhang zwischen elliptischen Modulfunktionen und indefiniten quadratischen Formen*, no. 22 in *Mathematische Werke*, p. 418–427, Göttingen, 1983.

[2] E. Hecke, *Zur Theorie der elliptischen Modulfunktionen*, no. 23 in *Mathematische Werke*, p. 428–460, Göttingen, 1983.

[3] A. Polishchuk, *Indefinite theta series of signature* $(1, 1)$ *from the point of view of homological mirror symmetry*, preprint math.AG/0003076.